Computational Complexity

Practice Exam

Definition 1. Let L be a language. We say that L is *length-decreasing self-reducible* if there is a polynomial-time oracle TM M such that for each $x \in \{0,1\}^*$:

$$x \in L \quad \text{if and only if} \quad M^L(x) = 1,$$

and the computation of $M^L(x)$ only queries L on strings of length strictly less than $|x|$.

Question 1 (2pt)**.** Let L be a language such that $L \subseteq \{1\}^*$. Prove that L is in P if and only if L is length-decreasing self-reducible.

Question 2 (1pt)**.** Consider the following language K, that consists of all strings x encoding a propositional formula φ, containing the propositional variables $p_1, \ldots, p_m$, such that there is a truth assignment $\alpha : \{p_1, \ldots, p_m\} \to \{0,1\}$ for which holds:

- there exist i, j such that $\alpha(p_i) \neq \alpha(p_j)$, and
- α satisfies φ.

Prove that K is NP-complete.

Definition 2. Let $L_1, L_2 \subseteq \{0,1\}^*$ be languages. We define the *concatenation* $L_1 \circ L_2$ of L_1 and L_2 as follows:

$$L_1 \circ L_2 = \{\ x_1 x_2 \mid x_1 \in L_1, x_2 \in L_2\ \}.$$

That is, $L_1 \circ L_2$ contains all strings x that can be split into two strings x_1 and x_2 such that $x_1 \in L_1$ and $x_2 \in L_2$.

Question 3 $(1 + 1 + 1$pt$)$**.** Prove that:

(a) NP is closed under union, i.e., if $L_1, L_2 \in$ NP then $L_1 \cup L_2 \in$ NP.

(b) NP is closed under intersection, i.e., if $L_1, L_2 \in$ NP then $L_1 \cap L_2 \in$ NP.

(b) NP is closed under concatenation, i.e., if $L_1, L_2 \in$ NP then $L_1 \circ L_2 \in$ NP.

Definition 3. A set $S \subseteq \{0,1\}^*$ is called *sparse* if it has polynomial density, i.e., if there exists a constant c such that for each $n \in \mathbb{N}$:

$$|S \cap \{0,1\}^n| \leq n^c + c.$$

We use SPARSE to denote the class of all sparse sets.

Question 4 (2pt)**.** Let $L \subseteq \{0,1\}^*$ be a language. Prove that $L \in \mathrm{P/poly}$ if and only if $L \in \mathrm{P}^{\mathrm{SPARSE}}$.

- *Hint:* Use a sparse set S to encode the advice, and vice versa. Remember to prove the implication clearly in both directions.

Definition 4. Define ZPP to be the class of languages L for which there is a constant c and a polynomial-time TM M which outputs either 0, 1 or ?, such that for all $x \in \{0,1\}^*$:

$$\Pr_r[M(x,r) = ?] \leq 1/2,$$
$$\text{if } M(x,r) = 1, \text{ then } x \in L, \text{ and}$$
$$\text{if } M(x,r) = 0, \text{ then } x \notin L,$$

where r is drawn from the uniform distribution over $\{0,1\}^{|x|^c}$. To get ZPP^O, one replaces the above M by the oracle TM M^O.

Question 5 $(2 + 2\text{pt})$**.** Prove that:

(a) The above definition of ZPP is equivalent to the definition of ZPP given in the book. That is, a language L meets the definition above if and only if it meets the definition of ZPP given in the book (Definition 7.7).

(b) $\mathrm{ZPP}^{\mathrm{ZPP}} = \mathrm{ZPP}$.